CHAPTER

# 15

# NETWORK MONITORING AND TUNING

**After reading this chapter and completing the exercises you will be able to:**

- Establish network benchmarks
- Install Network Monitor Driver
- Install, configure, and use Network Monitor, including setting up filters and triggers
- Install and configure the SNMP service
- Use System Monitor to monitor a network
- Troubleshoot and tune a network

Monitoring a network is as important as monitoring servers on the network. Network monitoring enables you, as an administrator, to quickly identify and fix problems and to determine when to upgrade a network to match growing needs. One important reason to gather network benchmarks and to monitor the network on an ongoing basis is so that you can differentiate between problems created by servers and workstations and those created by network difficulties. If administrators do not regularly monitor a network, it might be possible, for example, to mistakenly upgrade hubs or routers when the real problems are with servers or workstations, such as overloaded servers or slow NICs.

In this chapter, you learn how to use Network Monitor and System Monitor to identify network problems and differentiate them from server or workstation problems. You learn how to establish network benchmarks and how to monitor networks in different ways, as well as how to install network monitoring utility software such as Network Monitor, Network Monitor Driver, and the SNMP service. All of these tools will prove to be critical to you, particularly as your servers and the network grow more complex.

## Network Monitoring

Networks can be very dynamic in terms of changing patterns of communication. One minute a network may be running smoothly with no delays, and the next minute there are network slowdowns. Regularly monitoring your network is vital, because there are many factors that can influence network performance. For example, a network may experience slow traffic because of a defective cable or hub. Another source of problems can be a malfunctioning NIC on a server or workstation that creates bottlenecks by endlessly sending broadcasts over the network. In some cases, a server NIC may be performing normally, but may be too slow for the number of clients it must handle. Similarly, the network may be working normally, but appear to be slow because of a server that has a slow processor that causes network clients to wait in line.

Another reason why network activity changes is that client activity changes on the basis of times of the day and days of the week. For example, a segment of a college's network in the administration building may experience intense activity at certain times such as when the college is preparing its annual budget or working to finalize the payroll. A small architectural firm may experience heavy network activity when architects are completing large graphics files to submit to one or more clients.

Because networks are so dynamic, the best way you can prepare for and resolve problems is to monitor the network. Network monitoring is also more meaningful when you establish network benchmarks, so that you have a way to determine what network conditions are normal and what conditions indicate problems or the need to expand or upgrade the network. To establish network benchmarks, consider monitoring for the following:

- Slow, average, and peak network activity in relation to the work patterns at your organization
- Network activity that is related to specific protocols, such as TCP/IP and IPX/SPX
- Network activity that is related to specific servers and host computers
- Network activity that is related to specific workstations
- Network activity on individual subnets or portions of a larger network
- Network traffic related to WAN transmissions
- Network traffic created by particular software, such as client/server and multimedia applications

Plan to use your network benchmarks, along with the server benchmarks discussed in Chapter 14, as critical tools in helping you to tune the network and servers for optimum performance, as well as to quickly identify problems. For example, these benchmarks will help you determine if a slowdown reported by users is caused by a problem at a server or by a network problem, such as a broken network hub or switch.

## Windows 2000 Server Network Monitoring

There are four key network management and monitoring tools available in Windows 2000 Server:

- Network Monitor Driver
- Network Monitor
- SNMP service
- System Monitor

Network Monitor Driver enables server and workstation NICs to capture network performance statistics that are used by the Network Monitor and System Monitor tools. The SNMP service is used with specialized network monitoring systems to gather wide-ranging network data and to manage network devices. All of these tools are explained in the sections that follow.

## Using Network Monitor Driver

**Network Monitor Driver** is a protocol that works along with Network Monitor to enable you to monitor a network. **Network Monitor** is a Microsoft tool that captures and distills network performance information. When you install Network Monitor Driver on a server or workstation, it enables that computer's NIC to collect statistics about network performance, such as the number of packets sent and received at that computer. When Network Monitor Driver is installed, it links up with Microsoft's NDIS (Network Driver Interface Specification, see Chapter 3) on the computer in what is called the **local-only mode**, which captures and views only the contents of frames and packets sent to and transmitted from the local computer. This is in contrast to the **promiscuous mode** used by some network monitors and devices, in which the contents of all frames and packets are captured for possible viewing. With Network Monitor Driver loaded, the NIC gathers information about protocol traffic and network utilization, and data concerning broadcasts, unicasts, and multicasts. **Broadcasts** are transmissions sent to all locations of a network, for example, when a server or workstation sends a periodic broadcast that it is connected and working. A **unicast** transmission (see Chapter 3) involves sending one copy of each packet to each targeted destination. Thus, if eight workstations are requesting a multimedia application from a server, the server sends eight copies of each packet, one copy for each workstation—a transmission method that can generate considerable network traffic. **Multicasts** enable a multimedia server to make one transmission to a group of designated computers, which means that if eight computers request a multimedia application, only one packet is sent per transmission to the eight computers as a group.



A Windows 2000 workstation or server running Microsoft analysis software, such as Network Monitor or System Monitor, can connect to the computer running Network Monitor Driver and use that computer's NIC to capture data for analysis. Even computers remotely connected through RAS can be turned into network data collection stations. Figure 15-1

illustrates a computer running Windows 2000 Server, with Network Monitor and Network Monitor Driver loaded, obtaining data from a computer running Windows 2000 Professional in another location on the same network and from a computer running Windows 2000 Professional that is connected to a branch network and that has dialed into the main network through a RAS connection. Both computers running Windows 2000 Professional have Network Monitor Driver installed and the server that has Network Monitor can gather network performance data via the NICs on those computers.

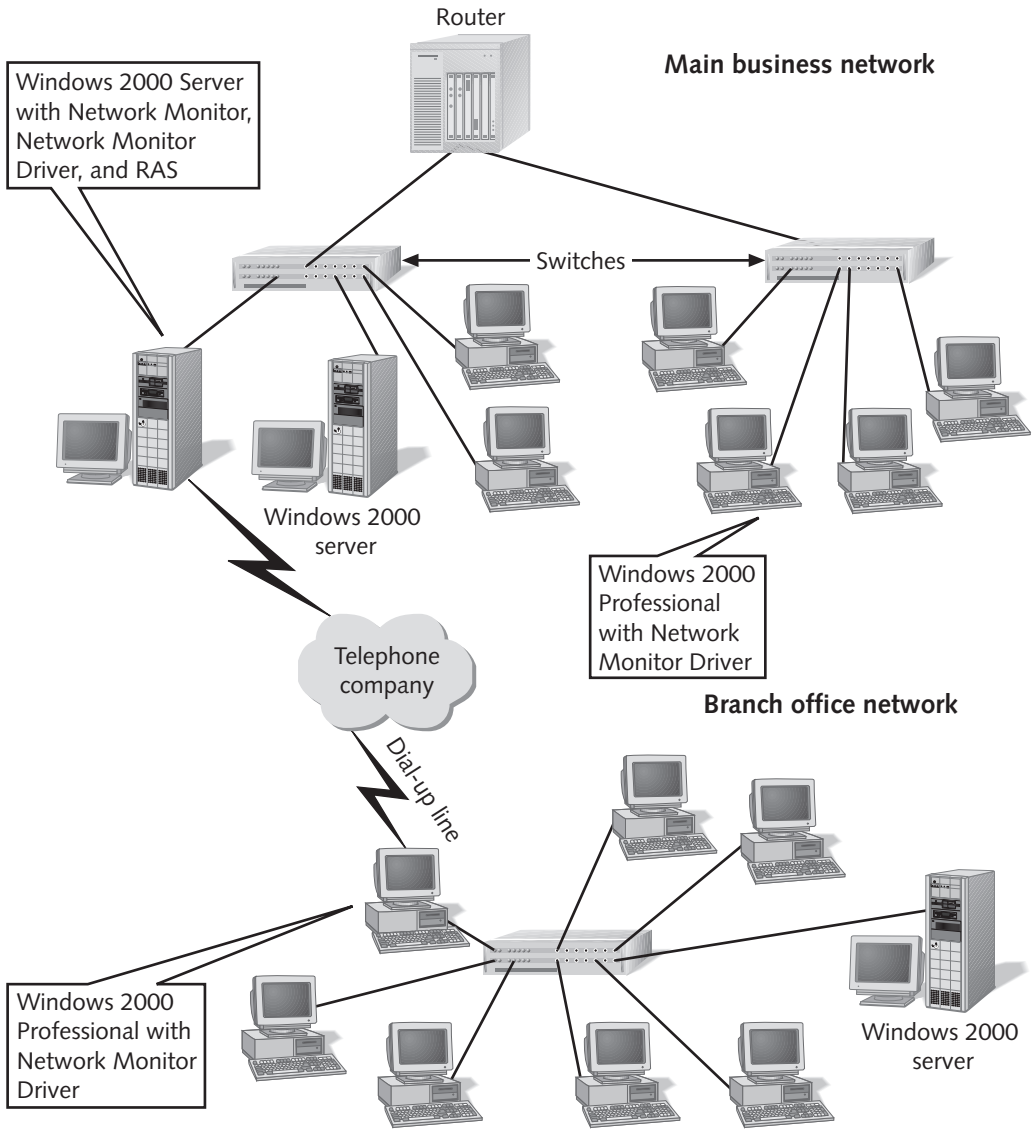


**Figure 15-1** Using Network Monitor Driver to gather network performance information on two separate networks


Windows 2000 Server comes with a version of Network Monitor Driver that works only on computers running Windows 2000 (Professional, Server, Advanced Server, and Datacenter). If you want to use other workstations as network data collection agents, such as those running Windows 95, Windows 98, or Windows NT, then it is necessary to purchase Microsoft Systems Management Server, which includes versions of Network Monitor Driver for these operating systems.

Network Monitor Driver is installed in Windows 2000 Server by using the Network and Dial-up Connections tool. Click Start, point to Settings, click Network and Dial-up Connections, right-click Local Area Connection, click Properties, click Install, double-click Protocol, and double-click Network Monitor Driver (see Figure 15-2). The Network Monitor Driver installation does not also install Network Monitor, which is installed separately as described later in this chapter. Try Hands-on Project 15-1 to install Network Monitor Driver.

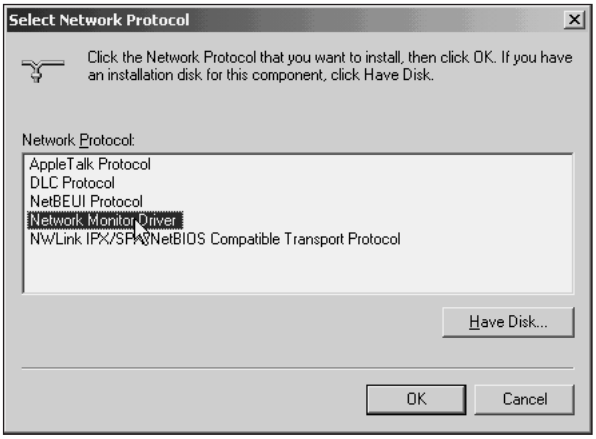


**Figure 15-2** Installing Network Monitor Driver



## USING NETWORK MONITOR

Network Monitor is included with the Windows 2000 Server CD-ROM and uses Network Monitor Driver to monitor the network from the server's NIC. When Network Monitor is installed, it enables you to monitor a full range of network activity and to check for possible problems. Network Monitor tracks information such as the following:

- Percent network utilization
- Frames and bytes transported per second
- Network station statistics
- Statistics captured during a given time period

- Transmissions per second information
- Information about broadcast, unicast, and multicast transmissions
- NIC statistics
- Error data
- Addresses of network stations
- Network computers running Network Monitor and Network Monitor Driver

When you run Network Monitor to monitor traffic across a network, Network Monitor Driver detects many forms of network traffic and captures packets and frames for analysis and reporting by Network Monitor. Since it operates in the local-only mode, only the contents of packets and frames sent to and from the server can be viewed. However, all packets and frames that pass through the server's NIC are monitored (although not all contents are viewed) so that it is possible to determine basic information about the network, such as the amount of traffic, the types of packets, and the source and destination addresses of computers transmitting data.


The version of Network Monitor that is included on the Windows 2000 Server CD-ROM is only designed to capture data at the server's NIC. Consider purchasing Microsoft Systems Management Server, which comes with a version of Network Monitor that can connect to and monitor activity from a NIC on any network computer that has Network Monitor Driver installed.

The general steps for installing Network Monitor are as follows (try Hands-on Project 15-2):

1. Open the Control Panel Add/Remove Programs tool.
2. Click Add/Remove Windows Components. If the Windows Components Wizard dialog box is not automatically started, click the Components button to start it.
3. Double-click Management and Monitoring Tools in the Windows Components Wizard dialog box.
4. Check Network Monitor Tools (see Figure 15-3) and click OK.
5. Click Next.
6. If requested, insert the Windows 2000 Server CD-ROM and click OK. (If a second dialog box is displayed, provide the path to the \I386 folder on the CD-ROM and click OK again.)
7. Click Finish.
8. Close the Add/Remove Programs window.

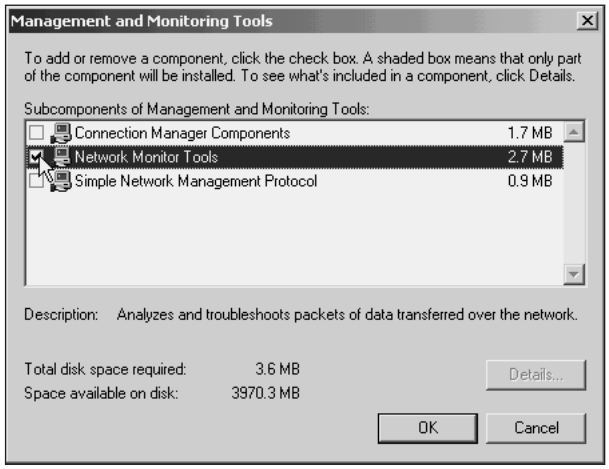


**Figure 15-3** Installing Network Monitor tools

The steps for starting Network Monitor are as follows:

1. Click Start, point to Programs, point to Administrative Tools, and click Network Monitor.
2. Click OK if there is an information box that reminds you to select the network to monitor or to use the local area network as the default, and then click the network you want to monitor in the *Select a network* dialog box.
3. Maximize one or both Network Monitor screens, if the display is not maximized.
4. Click the Start Capture button on the button bar to start capturing network performance data.
5. View the data displayed on the screen, such as % Network Utilization or the Network Statistics (see Figure 15-4).
6. Use the scroll bars in each of the four windows to view the information they offer.
7. If you want to pause capturing data, click the Pause button on the button bar, and click it again later to resume capturing. When you are finished, click the Stop Capture button on the button bar.
8. Close Network Monitor.
9. If the Save File dialog box is displayed, click Yes if you want to save the captured data in a file, or click No if you do not want to save the data. If you click Yes, specify the filename in which to save the captured data, and then click Save.

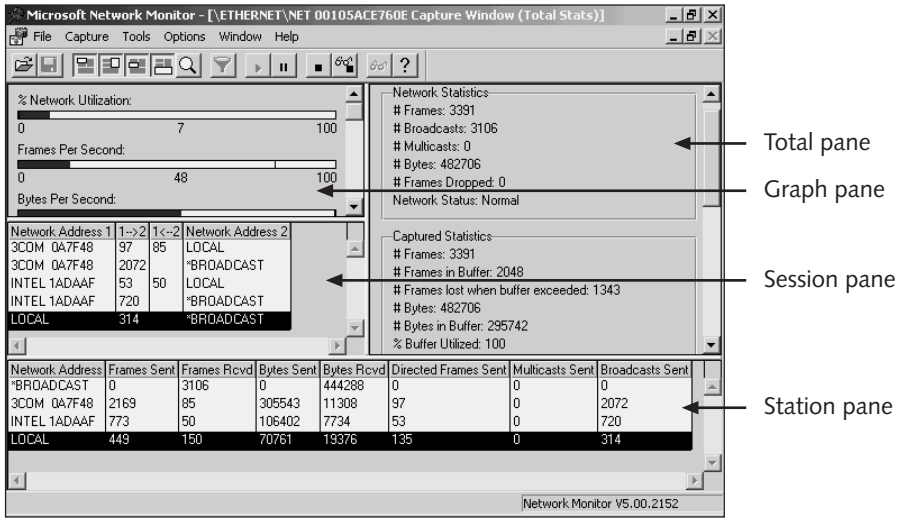


**Figure 15-4** Network Monitor capturing data


Both Network Monitor and System Monitor create a load on the CPU of the computer where they are running. When you implement these as a server administrator, plan to run them on a limited basis from a server, so that time spent gathering the data does not interfere with the server's other activities. Some server and network administrators run Windows 2000 Professional on their personal workstation and gather network data from there, using the workstation's NIC, or by briefly attaching to a server's NIC.

Network Monitor can be customized to present many different pictures of network activity, because it displays four panes of data and because **filters** (explained in the next section) can be set to collect specific types of information. The four panes (see Figure 15-4) and the information that they record are presented in Table 15-1. Filters can be built based on addresses, protocols, and properties. For example, you might create a filter to capture only information about IP activity or only IPX transmissions. You can choose to capture data for a short or long period of time.

**Table 15-1** Network Monitor Panes

| Pane | Information Provided in the Pane |
|---|---|
| Graph | Provides horizontal bar graphs of the following: % Network Utilization, Frames Per Second, Bytes Per Second, Broadcasts Per Second, and Multicasts Per Second |
| Total | Provides total statistics about network activity that originates from or that is sent to the computer (station) that is using Network Monitor and includes many statistics in each of the following categories: Network Statistics, Capture Statistics, Per Second Statistics, Network Card (MAC) Statistics, and Network Card (MAC) Error Statistics |

**Table 15-1** Network Monitor Panes (continued)

| Pane | Information Provided in the Pane |
|---|---|
| Session | Provides statistics about traffic from other computers on the network, including the MAC (device) address of each computer's NIC (see Chapters 2 and 3) and data about the number of frames sent from and received by each computer |
| Station | Provides total statistics on all communicating network stations, including: Network (device) address of each communicating computer, Frames Sent, Frames Received, Bytes Sent, Bytes Received, Directed Frames Sent, Multicasts Sent, and Broadcasts Sent |


The Session and Station panes only display up to 100 sessions at once. If your network has over 100 connected devices, you must view the devices 100 at a time by clicking the Capture menu and clicking Clear Statistics.

After you have captured a specific amount of data, you can view all of the captured information as a line-by-line report of each captured event by clicking the Stop and View Capture button on the button bar to display the screen shown in Figure 15-5.

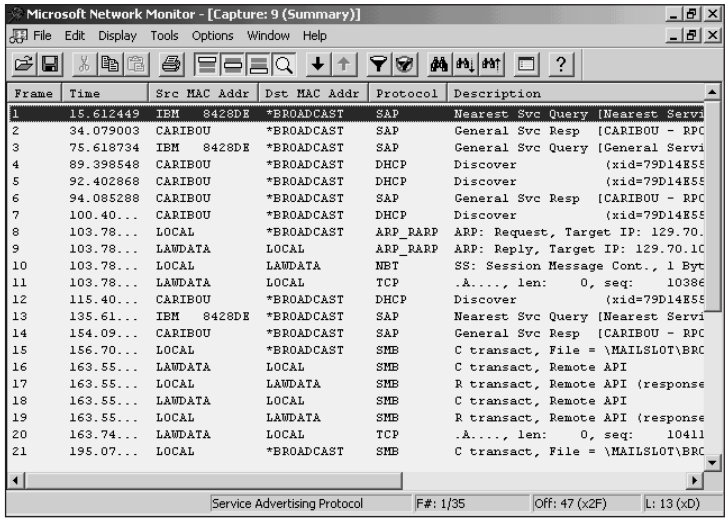


**Figure 15-5** Viewing capture summary data

Table 15-2 lists the information provided in the capture summary.

**Table 15-2** Capture Summary Window Information

| Column | Explanation |
|---|---|
| Frame | Shows the sequence of the frame as it was received, for example the first frame captured is 1, the second frame captured is 2, and so on |
| Time | Shows when the frame was captured in one of three formats: relative system time, when the frame was captured after capturing has been started, or when the frame was captured after capturing was stopped |
| Source MAC Address | Shows the device address of the sending computer |
| Destination MAC Address | Shows the device address of the receiving computer |
| Protocol | Shows the protocol used in the transmission |
| Description | Provides the description of the communication |
| Source Other Address | Shows other address information, such as an IP address or a computer name for the computer sending the frame |
| Source Other Destination | Shows other address information, such as an IP address or a computer name for the computer receiving the frame |
| Type Other Address | Defines the type of addresses shown in the Source Other Address and Source Other Destination columns, such as an IP address |

For example, if you wanted to review each transmission event from a server called Lawyer, you would click the Stop and View Capture button to see a capture summary window similar to the one shown in Figure 15-5. Next, you would click the Find (binoculars) button on the button bar, click the Address tab, which shows computer names and associates them with their MAC (device) addresses or IP addresses, click Lawyer as Station 1, click the double Direction arrow (< – >), click *ANY as Station 2 (see Figure 15-6), and click OK. You would then click the Find Next button on the button bar to locate the next transmission from Lawyer, and keep clicking the Find Next button to view all events associated with Lawyer, one at a time.

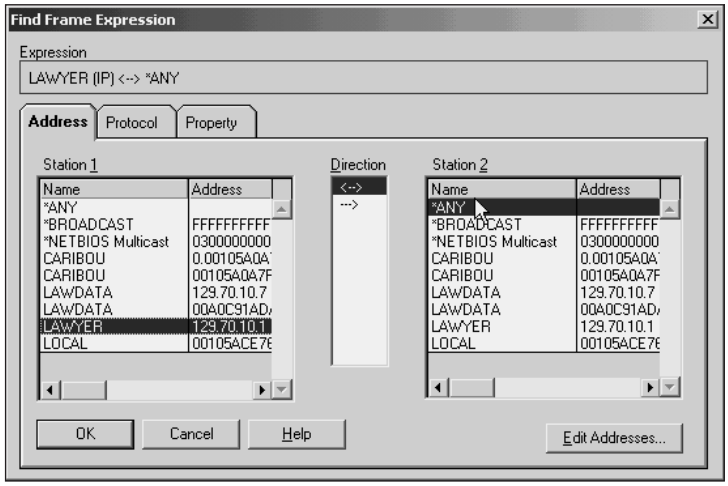


**Figure 15-6** Finding transmission events associated with Lawyer

Notice that in Figure 15-6, some computers, such as Caribou, have two names and addresses displayed in the Address tab. This means that these computers are configured to use two protocols. When you click one of these, the protocol associated with it is displayed in the Expression box on the tab. This can be a valuable tool for locating those computers that are configured to use protocols that are not needed, and then tuning the network for better performance by removing the unused protocols on those computers.

When you stop capturing data, you can save the capture summary data to a file by clicking the File menu, clicking Save As, providing a filename, and clicking Save. The default folder for saved capture information is \Winnt\System32\Netmon\Captures. Network Monitor is set by default to save up to 1 MB of information that is captured (you learn how to increase the capture capacity in the next section). After the information is saved, you can print the file contents, which provides a line-by-line listing of each captured event.

## Creating a Filter in Network Monitor

Network Monitor supports event management, which enables a server administrator to set up filters to capture a certain event or type of network activity. For example, the administrator may want to watch only activity between the server and a specific workstation. Another possibility is to track only IP activity related to Internet traffic into the server, or to track NWLink traffic between a NetWare server and a Windows 2000 Gateway for NetWare. The steps to set up a filter are as follows (try Hands-on Project 15-3):

1. Start Network Monitor from the Administrative Tools menu.
2. Click the Capture menu and click Filter (or click the Edit Capture Filter button on the button bar). Click OK if a warning is displayed that Network Monitor only captures information at the local computer.
3. Double-click the SAP/ETYPE (Service Access Point/Ethertype) line to specify a protocol to monitor (see Figure 15-7). Use the Disable All button to disable monitoring of the protocols, then select only the protocols you want to monitor and use the Enable button to allow capturing them (see Figure 15-8). Click OK after making your selections.



Network Monitor can filter frames and packets on the basis of two property types, Service Access Point (SAP) or Ethertype (ETYPE). SAP refers to the service access point, which specifies the network process that should accept a frame at the destination, such as TCP/IP, BPDU, and special manufacturers, including Novell (for IPX/SPX). ETYPE refers to a property of an Ethernet frame that includes a two-byte code for the protocol type and is used in Ethernet communications by many vendors (but is not a part of the Ethernet standard). You will find that for some protocols such as IP, you can choose from either property or monitor for both. If you are in doubt, monitor both types or select SAP, which conforms to the Ethernet standard.

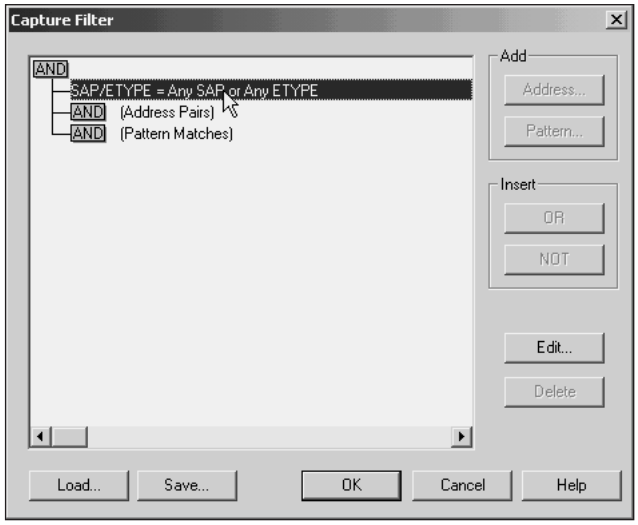


**Figure 15-7** Creating a filter

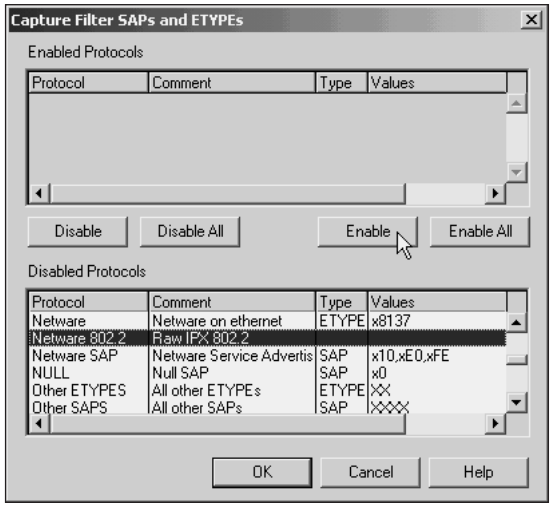


**Figure 15-8** Selecting a protocol to capture in a filter

4. Double-click (Address Pairs) (see Figure 15-7) to specify certain workstations or servers to include or exclude from monitoring. You can use the Direction option to monitor traffic one way or both ways between the stations you select to monitor. Click OK after your selections are complete.

5. Double-click the Pattern Matches option (see Figure 15-7) if you want to capture frames containing only certain types of data, read data from the beginning of a frame, or offset a designated number of bytes from the frame's beginning. A specific hexadecimal or ASCII pattern of data can be captured for study. Click OK.

6. Click OK again to return to the main Network Monitor screen and click the Start Capture button to start capturing data based on the filter you constructed.


Network Monitor cannot be actively capturing data when you create a filter. If the Capture menu Filter option (or the Edit Capture Filter button) is deactivated, then pause or stop capturing data until after you have configured the filter.

One common cause of a network slowdown or high network utilization is a bridge, switch, or a router set up in bridge mode that is saturating a network with too many bridge protocol data unit (BPDU) broadcasts because its rate of broadcasting is set at too small an interval between broadcasts. BPDUs are specialized frames used by bridges to exchange information with one another. You can create a filter to monitor the rate of BPDUs to help identify the device that is causing problems. To create the filter, click the Edit Capture Filter button in Network Monitor, double-click *SAP/ETYPE = Any SAP or Any ETYPE*, click the Disable All button, click BPDU in the Disabled Protocols box, click Enable, click OK, click OK again, and start capturing data.

Another example is a user who is sharing a large database with others, who access it over the network. You suspect that the database needs design improvements because each time users access it, they must load all tables in the database, and the result is degraded network performance. You can set up a filter that monitors all traffic to and from the workstation sharing the data. Click the Edit Capture Filter button, double-click (Address Pairs), make sure Include is selected, click the name of the workstation sharing the database in the Station 1 box, click the two-way arrow, click *ANY in the Station 2 box, click OK, click OK again, and start capturing data.

## Using a Capture Trigger



A **trigger** is used in Network Monitor as a way for you to have the software perform a specific function when a predefined situation occurs. For example, you can set up a trigger to stop a capture as soon as certain data is transmitted over the network or when the capture buffer is 100% full. The **capture buffer** is the amount of RAM and virtual memory that is used to store captured data. In another example, you might be tracking an intruder and want to trigger an audible alarm as soon as that intruder sends data over the network.

Consider a situation in which you want to start a capture using a filter, but for the sake of the server's performance, you want to stop the capture after the capture buffer is 25% full. To set the trigger, you would click the Capture menu, click Trigger, click the Buffer space radio button, leave 25% as the default, and click Stop Capture (see Figure 15-9). Try Hands-on Project 15-4 to practice creating a trigger.

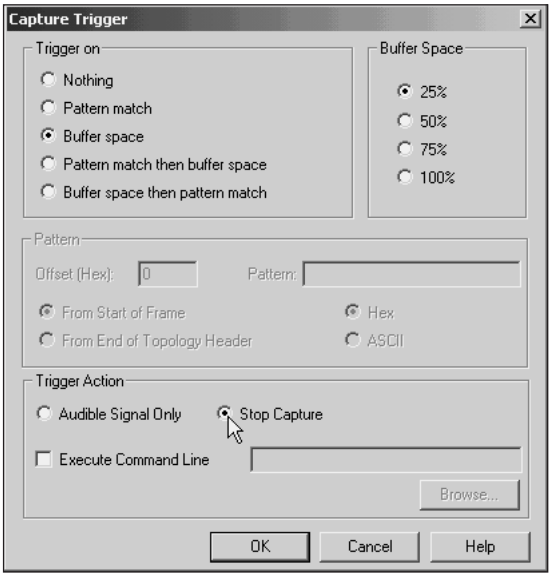


**Figure 15-9** Setting up a trigger


Increase the buffer size carefully, because it adds to the load on the server and may degrade other server operations. The capture buffer is set at 1 MB by default. You can increase the buffer size, when Network Monitor is not capturing data, by clicking the Capture menu and Buffer Settings.

## Using Network Monitor to Set Baselines

A basic way to establish network baselines from which to diagnose problems is to use information that you obtain from the Graph pane in Network Monitor. The data bars provide useful information that you can collect about network performance under light, medium, and heavy loads. Four of the most helpful statistics are the following (try Hands-on Project 15-5):

- *% Network Utilization:* Shows how much of the network bandwidth is in use
- *Frames Per Second:* Shows total traffic in frames for broadcasts, unicasts, and multicasts
- *Broadcasts Per Second:* Shows how much network traffic is the result of broadcasts from servers, workstations, and print servers
- *Multicasts Per Second:* Shows how much network traffic is due to multimedia servers

Begin gathering benchmarks on all four statistics so that you have an immediate understanding of what network load is typical. Also, be prepared to make adjustments in the network when even the typical statistics are high. For example, if % Network utilization is frequently over 40%, that means the network is experiencing collisions and there may be bottlenecks due to the network design, possibly indicating the need to create subnets. Network utilization that

is regularly over 60%–70% indicates a serious need to modify the network to address bottlenecks or increase network speed. Network utilization that is over 90% for a sustained period requires immediate attention in terms of locating the network problem or redesigning the network.

## Using Network Monitor to Diagnose Common Network Problems

Once you have determined baselines for your network's normal functions, Network Monitor can help you diagnose common network problems, such as:

- A failing NIC that is continuously broadcasting on the network
- Inefficient multimedia applications
- Problems with bridges, switches, or routers
- Problems with a particular workstation or section of the network
- An overloaded server

One indication of a network problem, often experienced as a network slowdown or as high network utilization, is when a device is continuously broadcasting, such as a failing NIC on a server or workstation. A dramatic increase in broadcasts per second along with an increase in network utilization is one indication that a device is malfunctioning. In this situation, you can use Network Monitor to help locate the computer that has the malfunctioning NIC. Use the Station pane to look for a network address (a NIC, NIC device address, or computer name) that is sending an abnormal number of broadcasts, such as several hundred or thousand, compared to all other stations.

If your network includes multimedia applications, then the Frames Per Second, Broadcasts Per Second, and the Multicasts Per Second statistics provide a way to establish information about the network load created by these applications. For example, if there are a high number of frames per second, a low number of broadcasts, and a low number of multicasts, then the multimedia application is likely employing unicasts. You might contact the multimedia application designers for information on tuning the application to use the more efficient multicasts. Or, if the application already uses multicasts, and both multicasts per second and network utilization are high, then consider increasing network bandwidth by increasing the speed of key network segments that are affected by multimedia applications. It may be necessary to upgrade several segments from 10 Mbps to 100 Mbps or more, for instance.



Another indication of a network problem is that the Frames Per Second indicator in the Graph pane of Network Monitor shows a dramatic increase. This may mean that a bridge, switch, or router set up to act as a bridge is flooding the network with frames and that it needs to be reset, reconfigured, or replaced.

A quick way to diagnose a problem at the NIC on a computer running Windows 2000 Server with Network Monitor is to view the Network Card (MAC) Error Statistics in the Total pane. Check for a high number of CRC (cyclic redundancy check) errors and dropped frames. Check the network connection to the NIC and repair any damage or consider replacing the NIC when these figures are high.

When you track activity to determine if a section of the network or a particular network workstation is having trouble receiving packets and frames, use the capture summary statistics (refer to Table 15-2). You can use the Find button to locate particular information, for example, by source and destination addresses to track transmissions and determine if particular transmissions are taking an excessive amount of time on the basis of when the transmission was sent from the source address and received by the destination address. If the time to one destination is excessive when compared to transmissions sent to other destinations, then this is an indication that there is a problem on the destination computer's network segment or that the destination computer has a slow or malfunctioning NIC. Also, you can use the capture summary information to look for situations in which the sending computer has to frequently resend frames and packets. This may indicate that the NIC or network connection at the source computer is having a problem because frames and packets are not constructed properly; or it may indicate that there is a problem at specific destinations. For example, if the source computer has to frequently resend frames and packets to all destinations, this indicates a problem at the source computer. If the source computer only experiences problems in communicating with a specific destination computer, then suspect a problem at the destination.

Another indication of a network problem is that the capture summary statistics reveal that a source computer must resend the same frame or packet several times. Frames and packets may be lost if retrys are over a certain value, such as five retrys, which is the default retry setting for TCP/IP. A high number of retrys indicates network bottlenecks or a serious problem on the network. For example, on a network that uses twisted-pair cable (10BaseTx) this may indicate that there is a problem in a network device such as a hub or switch. Often the problem is resolved by resetting or rebooting the device. On a network that uses coaxial cable (10Base2) the solution may be as simple as looking for a terminator that has been removed from one end of the network.

Yet another sign that there is a problem with a network device is that the capture statistics show a high number of session timeouts, indicating that a network device needs to be reset or perhaps is experiencing a bottleneck. For example, sometimes a network segment on a hub or switch will shut down automatically (called partitioning) when it determines there is a network problem. The solution is to fix the network problem, such as a defective NIC or cable, and then reset the segment on the hub or switch. Another possibility is that there is a need to upgrade the network device, for example, upgrading a hub to a switch or a switch to a router (depending on the network design).

Sometimes a server is so overloaded that it cannot respond to client requests in a timely way. You can determine this by tracing, in the capture summary data, how fast a server is able to respond to each client. You do this by looking at the time, source address, and destination address information. If the server is taking more time to respond than other network devices, then use System Monitor to determine why the server is overloaded (see Chapter 14). This is an example of both a server and a network problem because the overloaded server causes traffic delays in the network; however, the solution is to fix the server and not the network.

## Locating Unauthorized Users of Network Monitor

Network Monitor is a powerful tool and can create problems when it is employed by unauthorized users or network intruders. One of the most significant problems is that an unauthorized user can create a slowdown on a server by monitoring it from a remote location. You can immediately locate an unauthorized user by opening Network Monitor, clicking the Tools menu, and clicking Identify Network Monitor users. The resulting dialog box shows all of the Network Monitor users, including the computer name, account name, and network adapter device address (see Figure 15-10) of each user.

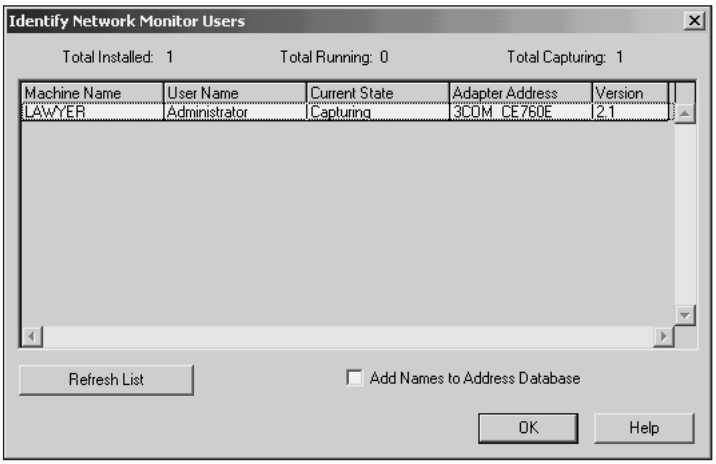


**Figure 15-10** Identifying all Network Monitor users

# Using the SNMP Service



A computer running Windows 2000 Server can be turned into an SNMP network data gathering agent by loading the SNMP service at that computer. The Simple Network Management Protocol (SNMP, see Chapter 3) is a protocol that enables computers and network devices to gather standardized data about network performance, and it is part of the TCP/IP suite of protocols. Although originally intended for use with TCP/IP, SNMP is now also compatible with IPX/SPX and AppleTalk. With the SNMP service loaded, a computer can communicate with an SNMP-based network management station (NMS) that obtains and distills data about network performance. SNMP uses two types of stations or computers, a network management station and network agents. The NMS monitors and manages network devices that are set up to use SNMP. The managed devices run agent software, such as Microsoft SNMP service, that is in contact with the network management station. Many devices connected to modern networks are SNMP agents, including computers, routers, hubs, switches, print servers, access servers, and UPSs.

SNMP enables three kinds of activities to be performed: monitoring a network, locating network problems, and managing network devices. When you install the SNMP service in

Windows 2000 Server, you enable the server to participate as an SNMP agent on a network. Also, while Microsoft SNMP is compatible with managing network devices, Windows 2000 Server does not include software that makes it a network management station. You must purchase that software through a third-party vendor. An NMS software package enables you to remotely manage and configure network devices, such as routers or switches, from a computer running Windows 2000 (preferably a Windows 2000 Professional workstation) that has SNMP installed.

Microsoft SNMP service provides support for management information base information gathering. A **management information base** (**MIB**) is a database of network performance information that is stored on a network agent, which gathers information for a network management station. A MIB stores parameters that can be configured remotely. A network management station can use a range of commands to obtain or alter MIB data. Because it is possible to use SNMP to configure network devices, it is important to establish a **community name** or string, which is a password that controls access to the MIB. Microsoft SNMP service is compatible with the original MIB-I standard plus the newer MIB-II standard. It is also compatible with SNMP versions 1 and 2. SNMPv2 provides greater security than the first version of SNMP and includes support for IPX/SPX and AppleTalk.

When there is a network management station set up on a network, the following Microsoft systems can be managed through SNMP:

- Windows 2000 and NT servers
- Windows 2000 and NT workstations
- WINS servers
- DHCP servers
- Internet Information Services servers
- Microsoft RAS and IAS servers

One immediate reason to install the SNMP service in Windows 2000 Server is that you can monitor the SNMP traffic using Network Monitor. For example, you can set up a Network Monitor filter to monitor SNMP activity. You might do this to make sure that there are no unauthorized users of NMS software who are trying to surreptitiously change security on devices such as routers. If you use a network management station to monitor network and SNMP-compliant devices, consider installing the SNMP service. You can install it from the Add/Remove Programs tool when you install Network Monitor or you can install it separately, by using the following steps:

1. Click Start, point to Settings, click Control Panel, and double-click Add/Remove Programs.
2. Click Add/Remove Windows Components. If the Windows Components Wizard dialog box is not automatically started, click the Components button to start it.
3. Double-click Management and Monitoring Tools in the Windows Components dialog box.

4. Check Simple Network Management Protocol (refer to Figure 15-3) and click OK.
5. Click Next.
6. Click Finish.

After you install the SNMP service, make sure that it is started, is set to start automatically, and is set up to have a community name. To check on all of these, click Start, point to Programs, point to Administrative Tools, and click Services. In the Status and Start-up type columns make sure that the SNMP Service is started and is set to start automatically. If you need to change either of these parameters, double-click SNMP Service and configure them on the General tab. If both parameters are already set appropriately, double-click SNMP Service anyway and click the Security tab. Check the *Accepted community names* box to make sure that the *public* community name is entered and that community rights are set to Read Only, so that no one else can change SNMP data on this Windows 2000 server (see Figure 15-11).

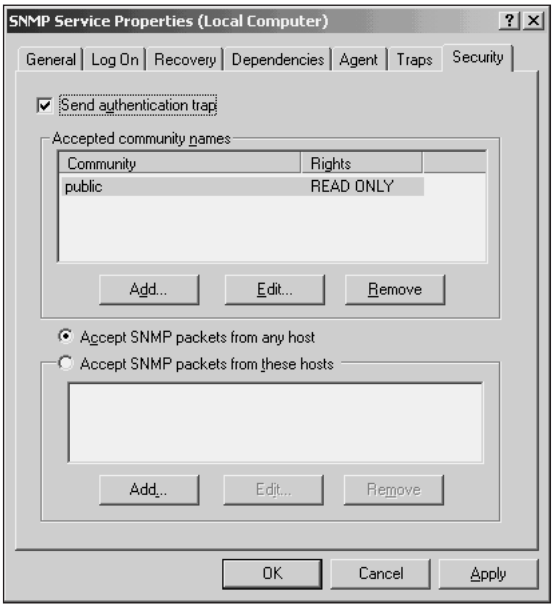


**Figure 15-11** Configuring the community name

If you purchase network management software, consider adding another community name so that you can manage Windows 2000 Server SNMP services using that software. To add another community name, click the Add button on the Security tab, enter the community name, specify the community rights, such as Read Write, and click Add (try Hands-on Project 15-6 to practice installing SNMP and setting a community name).

Microsoft SNMP service is also compatible with setting traps through a network management station. A **trap** is a specific situation or event that a network administrator may want to be warned about or to track, for example, when SNMP communications at the network management station detect that a network device is offline. The trap information is sent to

the network management station, which is identified by an IP or IPX address. To set up Microsoft SNMP service to enable a trap, click the Traps tab, enter a community name that is the same as the community name used for the trap set at the network management station, and enter the trap destination, which is the IP address of the network management station.


If you have a network management station or network management software and you want to set one or more traps related to a Windows 2000 server, then make sure that you also start the SNMP Trap Service and set it to start automatically. By default, this service is not automatically started. Use the Computer Management or Services tool in the Administrative Tools menu to check the status of the service.

## Using System Monitor for Network Monitoring

With Network Monitor Driver, Network Monitor, and SNMP service installed, several network-related monitoring objects can be used in System Monitor. This makes System Monitor another tool in your arsenal of network monitoring tools. Table 15-3 shows many of the network monitoring objects that are at your disposal.

**Table 15-3** System Monitor Network Monitoring Objects

| Object | Description |
|---|---|
| ICMP | Monitors network communication, using the Internet Control Message Protocol (ICMP), which is used by TCP/IP-based computers to share TCP/IP addressing and error information |
| IP | Tracks Internet Protocol (IP) activity and addressing (available if TCP/IP is installed in Windows 2000 Server) |
| NBT Connection | Monitors NetBIOS communications that are performed via TCP/IP data communication |
| NetBEUI | Tracks NetBEUI communications, such as communication errors, bytes sent, and data packets sent (available if NetBEUI is installed in Windows 2000 Server) |
| NetBEUI Resource | Monitors resources used, such as the data storage areas (buffers) used by a NIC transmitting NetBEUI data frames (available if NetBEUI is installed in Windows 2000 Server) |
| Network Interface | Tracks data that travels through the workstation or server NIC, such as the current bandwidth, the number of bytes transmitted and received, number of packets sent, and packet transmission and receipt errors |
| Network Segment | Monitors activity on the network segment to which the server or workstation is attached, such as broadcast and network utilization data (at this writing Network Segment is not fully implemented as an object in Windows 2000 Server, but expect it to be available as an update via Network Monitor Driver) |

**Table 15-3** System Monitor Network Monitoring Objects (continued)

| Object | Description |
|---|---|
| NWLink IPX | Tracks IPX communications sent to and from a Novell NetWare server or workstation, or an IPX-enabled print server (available only if NWLink is installed in Windows 2000 Server) |
| NWLink NetBIOS | Tracks NetBIOS communications over IPX, such as bytes sent, packet transmissions, and communication errors (available only if NWLink is installed in Windows 2000 Server) |
| NWLink SPX | Monitors SPX communications sent to or from a Novell NetWare server or workstation (available only if NWLink is installed in Windows 2000 Server) |
| TCP | Monitors TCP, including sent and received traffic and reset connections (available if TCP/IP is installed in Windows 2000 Server) |
| UDP | Tracks the User Datagram Protocol (UDP, see Chapter 3), which is the protocol used by network management stations, SNMP communications, and network agents for sending messages among themselves (available if TCP/IP is installed in Windows 2000 Server) |


Internet Control Message Protocol (ICMP, see Chapter 3) is a network maintenance protocol used within IP to assist in building information about routing network packets, including determining the shortest path to use for transmitting data. It also is used to help determine if a network station is live, to help locate network problems, and to reduce the flow of packets when the network is congested with traffic.

For those familiar with the Open Systems Interconnection (OSI) model for layered network communications, the objects and counters in System Monitor correspond to network operations at different layers (levels) of communication. You might associate the OSI layers as starting with the most basic functions, such as those related to electrical signals, and going up a layer at a time to more complex functions, such as those involving software. The most basic layer is the one at which the NIC and cable operate, called the physical layer. Next, is the data-link layer used by bridges and many switches. Some protocols, such as IP and devices such as routers, operate at an even higher layer (the network layer). TCP operates at the next higher layer, the transport layer, and programs, such as the Server service and My Network Places, operate at an even higher layers (the session, presentation, and application layers). Whether or not you are familiar with the OSI model, when you use System Monitor to track network activity or diagnose a problem, keep in mind that different objects and counters are related to different kinds of network communications.




If you are familiar with the OSI model, note that when you use network counters for different network objects in the Network Monitor, byte measurements are typically associated with the physical and data-link layers (NICs, cable, hubs, bridges, and switches), datagrams are associated with the network layer (such as IP traffic and routers), and segments are associated with the transport layer (TCP, UDP, and network device software drivers).

## Monitoring NIC and Server Activity

If you are tracking activity associated with a NIC, use the Network Interface object and the counters (representing the OSI physical layer): Bytes Received/sec, Bytes Sent/sec, and Bytes Total/sec. The instance that you track corresponds to the name of the NIC, such as 3Com EtherLink PCI. You can use this information to determine if the NIC is successfully transmitting and receiving, and the speed at which it is performing. If the NIC performance is below par when compared to other server or workstation NICs, use the Network Interface object and the Output Queue Length counter to determine if the computer is waiting for the NIC. The queue length should not be greater than 2, and if it is, consider upgrading the NIC driver (if it is out of date), adding a second NIC, or replacing the NIC with one that is faster (try Hands-on Project 15-7).

Another way to track activity through the NIC is to monitor the Server object and the counters: Bytes Received/sec, Bytes Transmitted/sec, and Bytes Total/sec. In addition to providing information about the NIC's performance, this data gives you an idea of the network activity at the server and if local bridges and switches are working normally.

Table 15-4 summarizes the Network Interface and Server counters.

**Table 15-4** Using System Monitor Objects and Counters to Monitor the NIC, Server, and Network Devices

| Object: Counter | Explanation |
|---|---|
| Network Interface: Bytes Received/sec | Measures the number of bytes received by the NIC per second and how fast the NIC converts a frame that is in the form of an electrical signal to one that can be processed as data. If your benchmarks show that this number is decreasing, there may be a problem in the NIC's ability to decode frames. |
| Network Interface: Bytes Sent/sec | Measures the number of bytes sent by the NIC per second and how fast the NIC encodes frames into electrical signals to place on the network. If your benchmarks show that this number is decreasing, there may be a problem in the NIC's ability to encode frames. |
| Network Interface: Bytes Total/sec | Measures the total number of bytes sent and received by the NIC per second, including the speed of encoding and decoding frames. If your benchmarks show that the speed represented by Bytes Sent/sec and Bytes Received/sec are about equal, but the Bytes Total/sec has decreased, check the local hubs, bridges, or switches to make sure they are working normally, and if these devices are fine, consider replacing the NIC, which may be slow or malfunctioning. |
| Server: Bytes Received/sec | Measures incoming bytes processed by the server per second. You can use this figure to set benchmarks and look for sudden decreases in traffic related to problems at the server's NIC or at a local hub, bridge, or switch. |
| Server: Bytes Transmitted/sec | Tracks the number of bytes that the server has placed on the network per second. Also consider using this as a benchmark. If this number starts to decrease compared to bytes received, and continues to decrease, it may mean that the server is gradually becoming overloaded. |
| Server: Bytes Total/sec | Measures the incoming and outgoing bytes and can be used to benchmark network activity at the server as well as server performance |

## Monitoring Protocol Activity

Protocol communications are analyzed by selecting objects that correspond to the protocol. For example, you can monitor IP traffic by using the IP object and the counters: Datagrams Received/sec, Datagrams Sent/sec, and Datagrams/sec. Similarly, if you are tracking NetBEUI traffic, use the counters: Datagrams Received/sec, Datagrams Sent/sec, Datagrams/sec, and Bytes Total/sec. Use these objects and counters to help you establish network benchmarks (try Hands-on Project 15-8). Also, if network traffic, such as IP traffic, is unusually heavy on the network or on a portion of the network, you may need to upgrade devices or increase the bandwidth. Another way to monitor TCP/IP-based traffic and develop benchmarks is to monitor the TCP object and the counters: Segments Received/sec, Segments Sent/sec, and Segments/sec.

You can use the System Monitor IP object and Fragmentation Failures counter to determine if there is a malfunctioning network device that is not correctly fragmenting packets and thus those packets are dropped. Packets are fragmented (broken up and resized) when they go from one type of network to another (on networks that use different packet sizes, such as a LAN connected to a WAN). Also, you can cross-check for a network device problem by monitoring the TCP object and the Segments Retransmitted/sec counter. A high rate of retransmitted segments indicates a network problem, possibly with a network device or a NIC.

Table 15-5 summarizes ways to use System Monitor to track protocols.

**Table 15-5** Using System Monitor Objects and Counters to Monitor Protocols

| Object: Counter | Explanation |
|---|---|
| IP: Datagrams Received/sec, Datagrams Sent/sec, and Datagrams/sec | These objects measure the IP datagrams (an IP datagram with an encapsulated TCP segment forms a packet) sent and received. Use these to establish benchmarks and to signal problems. For example, if there is a dramatic decrease in Datagrams Received/sec, check to determine if there is a problem with a router or Layer 3 (network layer) switch. |
| TCP: Segments Received/sec, Segments Sent/sec, and Segments/sec | These objects measure the TCP segments inside IP datagrams and can be used to establish benchmarks. There should be a one-to-one correspondence between IP datagrams and TCP segments or there may be a problem in how packets are being encoded or decoded at a device, possibly resulting in dropped packets. |
| IP: Fragmentation Failures | Measures the number of datagrams that are not being broken apart and resized for transmission across different networks. A high rate of these errors indicates a problem with a network device, such as a router. |
| TCP: Segments Retransmitted/sec | Measures the number of TCP segments that must be resent, such as segments that are dropped or IP datagrams that are not properly fragmented and reassembled, possibly indicating a problem at a router or NIC. |

## Monitoring for Network Utilization and Bottlenecks

On systems that have the Network Segment object, use this object to collect network benchmarks, using the counters: % Network Utilization and Broadcast Frames/sec. Also, as is true when you are monitoring with Network Monitor, network utilization that, on average, reaches over 40% indicates a busy network, 70% indicates a serious need for network analysis and troubleshooting, and utilization that is typically over 90% indicates a problem requiring immediate attention.

If you detect a bottleneck at a server by using either Network Monitor or System Monitor, you can use System Monitor to determine if the bottleneck is caused by a software problem at the server, for example, if the Server or Workstation services are down or hung (also see Chapter 14). Use the Server object and the Errors System counter, which should have zero to only a few errors. If there are errors, this indicates that an important service, such as the Server or Workstation service, is not working. Another indication that there is a problem with the Server or Workstation service is that the Server object and the Sessions Errored Out counter shows a high value (some sessions may error out because the server times them out normally, but this number should only be 1 or 2). Table 15-6 presents a summary of objects and counters used in monitoring the server and network for bottlenecks.

**Table 15-6** Using System Monitor Objects and Counters to Monitor Server and Network Bottlenecks

| Object: Counter | Explanation |
|---|---|
| Network Segment: % Network Utilization | Measures what percentage of the network bandwidth is in use—40% reflects a busy network, 70% signals a significant problem, such as a NIC or bridge saturating the network, over 90% requires immediate action to locate the source or sources of network bottlenecks |
| Network Segment: Broadcast Frames/sec | Tracks the number of broadcast frames sent per second and can be used to help establish network benchmarks as well as find a network station that is sending an abnormal number of broadcasts (including the server) |
| Server: Errors System | Measures for system service problems at the server and reflects a bottleneck, that may indicate that a critical service is not started, such as the Workstation or Server service. Suspect a problem when this value is over 0 or 1 |
| Server: Sessions Errored Out | Measures the number of server sessions that have terminated due to errors and can indicate a problem connecting to the server or in accessing a critical server service—troubleshoot a server problem if this number is frequently over 2 |

## Monitoring Web and FTP Services

The System Monitor offers a way to study the impact of Web services on a Windows 2000 server. When IIS is installed to perform as a Web server, you can use the Web Service object and several associated counters to study Web activity. For example, if you want to study the

number of current Web server connections, use the Current Connections counter to track the connectivity data over time. You might add the counter, Total Files Sent, to get additional information about how many Web pages users are accessing. The Maximum Connections counter enables you to track how often the total number of users reaches the maximum connection count, so that you can determine if the maximum should be raised or lowered.

One way to monitor the impact of running IIS on the server processor and on the network is to simultaneously monitor the following objects and counters:

- Web Service object and the Bytes Received/sec counter
- Web Service object and the Bytes Sent/sec counter
- Web Service object and the Current Connections counter
- Process object, % Processor Time counter, and the IIssrv instance

If you are running IIS FTP services, there is an FTP Service object that has many counters that are similar to those available for Web services. For example, you can monitor file transfer activity by using the FTP Service object and the following counters:

- Total Files Received
- Total Files Sent
- Total Files Transferred

To get a better picture of the file sizes and network activity, add two more counters to your monitoring: Bytes Received/sec and Bytes Sent/sec. Also, equate this data with the number of users by monitoring the FTP Service counter, Current Connections. Table 15-7 summarizes System Monitor objects and counters used to monitor Web and FTP servers.

**Table 15-7** Using System Monitor Objects and Counters to Monitor a Web Server

| Object: Counter | Explanation |
|---|---|
| Web Service: Current Connections | Measures the number of users currently logged on to the IIS Web services. Use this to create Web server benchmarks and to test the user load on the server. |
| Web Service: Maximum Connections | Tracks the maximum number of users who have been connected during the time of monitoring; it can be used to help you understand when to tune the server, for example, to increase the maximum number of users, to create more bandwidth, and to upgrade the server. |
| Web Service: Bytes Received/sec counter | Measures the incoming bytes processed by the Web server per second. You can use this figure to set benchmarks and look for sudden decreases in traffic related to problems at the server's NIC or at some point on the network. |
| Web Service: Bytes Sent/sec counter | Measures the number of bytes that the Web server has placed on the network per second. You can also use this as a benchmark. If this number starts to decrease compared to bytes received, and continues to decrease, it may mean that the server is overloaded, for example, requiring a faster processor and more L2 memory. |

**Table 15-7** Using System Monitor Objects and Counters to Monitor a Web Server (continued)

| Object: Counter | Explanation |
|---|---|
| FTP Service: Total Files Received, Total Files Sent, and Total Files Transferred | Measure the file activity generated by users; they can be used to establish benchmarks for FTP file activity |
| FTP Service: Bytes Received/sec, Bytes Sent/sec, Bytes Total/sec | Measure the network activity at the FTP server; they can be used to establish benchmarks |

## Monitoring SMTP Services

When IIS is configured for SMTP Services, the System Monitor SMTP Server object provides a way to monitor SMTP. There are a full range of counters that enable you to monitor messages that are received and sent, such as Messages Received Total, Messages Sent/sec, Messages Delivered Total, Messages Delivered/sec, Local Queue Length, % Recipients Local, and % Recipients Remote. These counters enable you to track activity on the SMTP server and to identify problems. To identify message-sending problems you can study any of the Badmailed Messages counters, such as Badmailed Messages (Hop Count Exceeded) or check the Outbound Connections Refused counter. Table 15-8 summarizes the objects and counters used for monitoring SMTP services.

**Table 15-8** Using System Monitor Objects and Counters to Monitor SMTP Services

| Object: Counter | Explanation |
|---|---|
| SMTP Server: Messages Received Total | Measures total message traffic into the server and can be used to establish benchmarks |
| SMTP Server: Messages Delivered Total | Measures the total message traffic out of the server and can be used to establish benchmarks |
| SMTP Server: Local Queue Length | Shows the number of messages in the local SMTP message queue. If users report that they are not receiving e-mail, monitor this object:counter combination. The message queue length should reflect constant change as it processes and routes messages. If the length does not change, suspect that the queue or the service is hung. Check to make sure that the Simple Mail Transport Protocol (SMTP) service is started and set to start automatically. Also, try stopping and restarting the service. |
| SMTP Server: Badmailed Messages (Hop Count) | Tracks the number of messages discarded because they went through more hops than specified, possibly indicating that the destination node is down or that there is a network problem between the SMTP server and the destination |
| SMTP Server: Outbound Connections Refused | Tracks messages turned down at a destination. A high number may indicate that someone at your site is randomly sending messages (spamming) or attempting surreptitious activities |

## Network Tuning Tips

Keep network performance at its optimum by looking for ways to tune the network. In general, some of the easiest and least expensive tuning activities include keeping network drivers up to date, setting the appropriate network access order on operating systems that support this kind of tuning, and making sure that servers are well outfitted to handle the load expected of them. The following list provides a summary of the ways in which you can tune a network:

- Make sure that NIC drivers are regularly updated, particularly on servers, but also on workstations, so that the most recent NIC drivers are in use.
- Replace older and slower NICs with faster ones (see Chapter 2).
- Tune the network access order, particularly on Windows NT and Windows 2000 workstations (as explained in Chapter 3 and illustrated in Hands-on Project 3-7).
- Implement TCP/IP exclusively, if possible, but in any case use only the minimum number of protocols required for network services.
- Make sure that all servers can keep up with the network traffic to them, by ensuring that the server specifications match the load placed on servers (see Chapter 2).
- Monitor for excessive BPDU broadcasts from bridges, switches, and routers set up to bridge, and reduce the frequency of broadcasts from these devices.
- Monitor the network for saturation from malfunctioning devices, such as NICs that are broadcasting excessively.
- Replace aging network equipment with newer, faster equipment, for example, replacing network hubs with faster switches or switches with routers.
- Replace multimedia applications that use unicasting with applications that perform multicasting.
- Upgrade network bandwidth (speed) to accommodate the network traffic that you detect from monitoring, for example, upgrading 10 Mbps network links to 100 Mbps or faster, particularly on networks that employ multimedia and client/server applications.



## Chapter Summary

- Monitoring your network is as important as monitoring a server, and in many cases, the interrelationship between network performance and server performance means that a conscientious administrator should regularly monitor both. One of the first places to start network monitoring is to establish benchmarks that reflect light, medium, and heavy network loading periods.
- Windows 2000 Server offers several powerful network monitoring tools: Network Monitor Driver, Network Monitor, the SNMP service, and System Monitor. Before you begin monitoring a network, plan to install Network Monitor Driver as the first step;

this turns a server's NIC into a device that can also capture network performance information. With Network Monitor Driver and Network Monitor installed, you are ready to establish network benchmarks. You can also monitor all kinds of network performance, such as network utilization, stations connected to the network, broadcasts, and statistics related to the Network Monitor host's NIC connection. System Monitor provides additional ways to monitor the network and offers the advantage that the server system can be monitored at the same time.

- The Microsoft SNMP service is provided for compatibility with SNMP-based network management stations and software used to monitor all kinds of networks, network equipment, and network situations. SNMP provides the ability to gather performance information and to manage network devices.
- Network monitoring is a critical tool to help you understand when to tune a network for optimum performance. In some cases, network monitoring can reveal simple and inexpensive steps you can take to improve performance.

In the next chapter, you learn ways to troubleshoot all kinds of server and network problems, such as connectivity, printing, security, and boot difficulties.

## Key Terms

**broadcast** — A transmission that sends one copy of each frame to all points on a network, regardless of whether a recipient has requested communication with the sender.

**capture buffer** — The amount of RAM and virtual memory that is used to store data captured by Network Monitor.

**community name** — In SNMP communications, a password used by network agents and the network management station so that their communications cannot be easily intercepted by an unauthorized workstation or device.

**filter** — A capacity in network monitoring software that enables a network or server administrator to view only designated protocols, network events, network nodes, or other specialized views of the network.

**local-only mode** — A process of capturing and viewing the contents of only the frames and packets sent to and transmitted from a specific networked computer's or device's NIC.

**management information base** (**MIB**) — A database of network performance information that is stored on a network agent, which gathers information for a network management station and that stores parameters that can be configured remotely.

**multicast** — A transmission method in which a server divides recipients of an application into groups, such as a multimedia application. Each data stream is a one-time transmission that goes to one group of multiple addresses, instead of sending a separate transmission to each address for each data stream. The result is less network traffic.

**Network Monitor** — A Windows NT and Windows 2000 network monitoring tool that can capture and display network performance data.

**Network Monitor Driver** — A software component that enables a Microsoft-based server or workstation NIC to gather network performance data for assessment by Microsoft Network Monitor.

**promiscuous mode** — The process of capturing and viewing the contents of all frames and packets sent across a NIC or network device, regardless of the destination of those frames and packets.

**trap** — A specific situation or event detected by SNMP that a network administrator may want to be warned about or to track via a network management station, for example, when a network device is unexpectedly down or offline.

**trigger** — A method used to have Network Monitor perform a specific function when a predefined situation occurs, for example, stopping a capture of network data when the capture buffer is 50% full.

**unicast** — A transmission method in which one copy of each packet is sent to each targeted destination; a transmission method that can generate considerable network traffic when compared to multicasting, when the transmission is a multimedia application.

## Review Questions

1. You want to use Network Monitor to monitor only NWLink traffic on a network. How can you do this?
   a. Create a trigger.
   b. Use the NWLink object.
   c. Create a trap.
   d. Create a filter.
2. You want to track each communication event associated with a computer named Henry. What monitoring tool enables you to do this type of tracking?
   a. System Monitor using the view report window
   b. System Monitor using the histogram mode and the Job Object Details object
   c. Network Monitor using the capture summary window
   d. Network Monitor using the Total window
3. You have opened Network Monitor, but it does not seem to be able to capture data from your server's NIC. Which of the following is the most likely cause?
   a. Network Monitor Driver is not installed.
   b. SNMP Service is not set up to enable traps.
   c. You have not previously run *netperf* in the Command Prompt window.
   d. all of the above
   e. only a and b
   f. only b and c

4. You have purchased a network management system and already have the network management station installed on your network. Today you are reviewing vendor statistics for switches and routers, because you plan to buy several new ones for the network. What network management feature should you look for in these devices?
   a. ability to operate as a backup NMS
   b. MIB compatibility
   c. SNMP compatibility
   d. all of the above
   e. only a and b
   f. only b and c
5. Your network has a workstation that is sending 20 times the number of broadcasts as other computers on the network. What steps should you take in this situation?
   a. Limit the times that the user can access the network.
   b. Begin troubleshooting by replacing that computer's NIC.
   c. Install network use accounting software, so that you can bill active users such as this more than users who are not as active.
   d. Replace the entire workstation with one that has a slower NIC and bus speed.
6. You want to use System Monitor to determine if the NIC on your Windows 2000 server is able to keep up with the speed of the server while servicing client requests. Which of the following System Monitor objects and counters should you use?
   a. IP object using the Datagrams Outbound No Route counter
   b. IP object using the Datagrams Forwarded/sec counter
   c. Network Interface object using the Current Bandwidth counter
   d. Network Interface using the Output Queue Length counter
7. Your network has several older bridges that seem to make the network operate slower. What should you monitor in this situation?
   a. Use Network Monitor to track BPDU traffic.
   b. Use Network Monitor to track all IP traffic.
   c. Monitor SNMP at those bridges, because they are using an older SNMP version that creates congestion.
   d. Monitor SMTP traffic at the bridges, because large mail messages are difficult to transmit through a bridge.
8. Network Monitor Driver is installed from which of the following?
   a. Control Panel Add/Remove Programs tool
   b. Control Panel Add/Remove Hardware tool using the install driver option
   c. Network and Dial-up Connections tool
   d. all of the above
   e. only a and b
   f. only a and c

9. After you install the SNMP service in Windows 2000 Server, what should you configure first in order to guarantee security?
   a. a trap
   b. a community name
   c. Set the SNMP version to SNMPv1.
   d. the MIB routing table
10. Network Monitor Driver operates in which of the following modes?
   a. promiscuous mode
   b. local-only mode
   c. investigative mode
   d. all of the above
   e. only a and c
   f. only b and c
11. Which of the following System Monitor counters and objects can you use to gather benchmarks on a TCP/IP-based network?
   a. the IP object using the Datagrams Received/sec, Datagrams Sent/sec, and Datagrams/sec counters
   b. the TCP object using the Segments Received/sec, Segments Sent/sec, and Segments/sec counters
   c. the Cache object using the Copy Read Hits % and Copy Reads/sec counters
   d. all of the above
   e. only a and b
   f. only b and c
12. You have been monitoring a network that normally has network utilization at 20%–30%, but during the past month the typical network utilization has risen to 75%. What should you do?
   a. Seventy-five percent represents an acceptable figure, and there is no need to do anything.
   b. Seventy-five percent is not a serious problem, but you should plan to examine how to tune network performance during the next couple of months.
   c. Seventy-five percent represents a serious problem, and you should begin more intense monitoring to locate problems and possibly upgrade portions of the network.
   d. Seventy-five percent means that a majority of your servers are overloaded and should be upgraded immediately.

13. Which of the following is(are) made possible by using SNMP?
    a. managing network devices
    b. monitoring a network and network devices
    c. locating network problems
    d. all of the above
    e. only a and b
    f. only b and c
14. Your boss was at a meeting this morning during which there were complaints that the Web server you manage often refuses connections because it seems to reach the maximum for connected users. How can you monitor this situation so that you can tune the Web server for the appropriate number of connections?
    a. Monitor the Web Service object and the Current Connections counter.
    b. Monitor the Web Service object and the Maximum Connections counter.
    c. Monitor the Processor object, the Creating Process ID counter, and the IISSrv instance.
    d. all of the above
    e. only a and b
    f. only b and c
15. You want to use Network Monitor to monitor the network while you are in a long morning meeting because that is the best time for you to capture the data you need. Unfortunately, you are worried that it may slow server performance if it runs for the duration of your meeting. What can you do?
    a. Temporarily excuse yourself in the middle of the meeting and pause the capture.
    b. For the sake of the server's performance, don't start the capture until you return.
    c. Set Network Monitor to run as a background process.
    d. Set a trigger to stop the capture when the capture buffer reaches 25% or 50%.
16. Network Monitor is installed from which of the following?
    a. Control Panel Add/Remove Programs tool
    b. Control Panel Add/Remove Hardware tool using the install driver option
    c. Network and Dial-up Connections tool
    d. all of the above
    e. only a and b
    f. only a and c

17. Your assistant needs to determine the device address of a workstation that is currently connected and transmitting on the network. Which of the following network monitoring tools can display the device address?
    a. System Monitor using the IP object
    b. Network Monitor using the Station or Session pane
    c. Network Monitor using the Total pane
    d. System Monitor using the NBT object
18. You want to create a filter in Network Monitor, but the Edit Capture Filter button is deactivated. What is the problem?
    a. You must set the Network Monitor properties to enable filtering.
    b. You must set the Network Monitor Driver properties to enable filtering.
    c. You can only create a filter in the Session pane, but you have deactivated that pane.
    d. Network Monitor is already capturing data, and you must pause or stop capturing.
19. The CIO of your company wants to monitor two remote networks, along with the main company network. All of the workstations on the remote networks are running Windows 2000 Professional and have RAS access to the main network. The main network includes servers running Windows 2000. How can you most easily monitor all three networks?
    a. Physically relocate two Windows 2000 servers from the main network, placing one server on each remote network, and then set up a Network Monitor and Network Monitor Driver on a server in each location.
    b. Set up all network servers and workstations as SNMP agents and purchase a network management system to monitor all three networks.
    c. Set up Network Monitor and Network Monitor Driver on at least one Windows 2000 server and install Network Monitor Driver on at least one workstation at each remote site.
    d. There are no Windows 2000 Server tools that enable networks to be monitored over RAS.
20. Your network has over 300 workstations presently connected, but Network Monitor displays information for only 100 workstations. What is the problem?
    a. You must configure Network Monitor Driver for over 300 connections.
    b. You must switch to using the Graph pane in Network Monitor.
    c. Click the Capture menu and click Clear Statistics to view the next 100.
    d. The version of Network Monitor that comes with Windows 2000 Server is only designed to monitor a maximum of 100 workstations. It is necessary to purchase the version of Network Monitor that is included with System Management Server in order to view over 100.

21. In Network Monitor, how might you view traffic from only one workstation, as a way to determine if that workstation is creating a network load?
    a. Create a trap using that workstation's IP address.
    b. Create a filter using that workstation as Station 1 and *ANY as Station 2.
    c. Use the Find utility in the capture summary.
    d. all of the above
    e. none of the above
    f. only a and b
    g. only b and c
22. Which of the following System Monitor objects will give you the best idea of the number of files sent and received over the network via FTP on your Web server?
    a. Web Service
    b. IP
    c. TCP
    d. FTP Service
    e. None of the above, because there are no System Monitor objects that track FTP activity (you must do this through Network Monitor).
23. The SNMP service is installed from which of the following?
    a. Control Panel Add/Remove Programs tool
    b. Administrative Tools menu, selecting the Services tool
    c. Network and Dial-up Connections tool
    d. all of the above
    e. only a and b
    f. only a and c
24. Your organization has 42 Windows 2000 servers and 7 of those servers house very modern multimedia applications that are used for instruction, information distribution, and specialized training. Which of the following should you monitor as a way to determine the network traffic created by the multimedia applications and learn if multimedia applications should be tuned?
    a. broadcasts compared to bytes sent per second and frames per second
    b. multicasts, broadcasts, frames per second, and network utilization
    c. broadcasts and network utilization
    d. segments sent per second compared to bytes sent per second

25. In general, when you establish network benchmarks, which of the following should you monitor?
    a. typical protocol traffic, such as TCP/IP traffic
    b. a typical connection session for every station on the network, regardless of the network's size
    c. periods representing slow, average, and peak network activity
    d. all of the above
    e. only a and b
    f. only a and c

## HANDS-ON PROJECTS


### Project 15-1

In this project you install Network Monitor Driver in Windows 2000 Server. Network Monitor Driver enables Network Monitor and System Monitor to gather network performance data via the server's NIC.

**To install Network Monitor Driver:**

1. Click **Start**, point to **Settings**, and click **Network and Dial-up Connections**.
2. Right-click **Local Area Connection**, and then click **Properties**.
3. Click the **Install** button.
4. Double-click **Protocol**. What protocols are listed in the Network Protocol box? Record your observations in your lab journal or in a word-processed document.
5. Double-click **Network Monitor Driver**. (If asked for it, insert the Windows 2000 Server CD-ROM and specify the path to the CD-ROM and \I386 folder, such as **D:\I386**. Click **Continue**.)
6. Record whether the driver appears in the Local Area Connection Properties box.
7. Click **Network Monitor Driver**. What description is displayed? Are there any properties to configure (is the Properties button activated)? Record your answers.
8. Click **Close**.


### Project 15-2

This project gives you the opportunity to practice installing Network Monitor. Make sure that Network Monitor Driver is installed before you start (refer to Hands-on Project 15-1).

**To install Network Monitor:**

1. Click **Start**, point to **Settings**, and click **Control Panel**.
2. Double-click the **Add/Remove Programs** icon.

3. Click **Add/Remove Windows Components**. If the Windows Components Wizard dialog box is not automatically started, click the Components button to start it.
4. Double-click **Management and Monitoring Tools** in the Windows Components dialog box. What are the tools that can be installed? Record this in your lab journal or in a word-processed document.
5. Place a check mark in the box in front of **Network Monitor Tools** (refer to Figure 15-3) and click **OK**.
6. Click **Next**.
7. If requested, insert the Windows 2000 Server CD-ROM and click **OK**. (If a second dialog box is displayed, provide the path to the \I386 folder on the CD-ROM and click **OK** again.)
8. Click **Finish**.
9. How can you check to make sure that Network Monitor is installed?


## Project 15-3

In this activity, assume that your network has an older NetWare server that runs a database application that uses NetWare's Service Advertising Protocol (SAP—do not confuse this with Service Access Point, which has the same acronym but is a different network concept). You want to create a filter to monitor only NetWare SAP frames that are received and sent by the NetWare server to determine if they are creating excessive network traffic.

**To create the filter to monitor only NetWare SAP frame traffic:**

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Network Monitor**. If a warning box is displayed that indicates a default network is not selected, click OK. Also, click OK if the Select Default Network dialog box is displayed (or select a network per your instructor's advice). (If you select a network, make sure that NET Dial-up Connection Capture Window is not displayed in the Network Monitor title bar—for capturing through the modem connection. If it is, and after Network Monitor starts, click the Capture menu, click Networks, click Local Computer, and double-click a selection that has the device address of the server's NIC instead of the modem.)
2. Does Network Monitor start capturing data as soon as you open the tool? How can you make sure that it is not capturing data? Record your observations.
3. Click the **Edit Capture Filter** button (it resembles a funnel) on the button bar. If the Capture Filter information box appears, warning that traffic is detected only at the local computer, click **OK**.
4. Double-click **SAP/ETYPE = Any SAP or Any ETYPE** (remember that here SAP means Service Access Point, refer to Figure 15-7).
5. What are some of the protocols that you can monitor? Record some examples in your lab journal or in a word-processed document.
6. Click the **Disable All** button.

7. Click **Netware SAP** (SAP here means Service Advertising Protocol) in the Disabled Protocols box, and then click the **Enable** button. Click **OK**.
8. Double-click **(Address Pairs)**.
9. What stations are included in the Station 1 and Station 2 boxes? In what directions can communications be tracked between stations in the two boxes? How would you set it up to view all traffic between only a NetWare server and all other stations on the network?
10. Although the default settings will monitor all traffic, practice setting up a relationship that monitors traffic from "*Any group" to "*Any" address on the network (even though these are already set up). Click the **Include** radio button. Click ***ANY GROUP** in the Station 1 box. Click the two-way arrows, **< – >**, in the Direction box and click ***ANY** in the Station 2 box. Click **OK**.
11. What relationship is now displayed under the (Address Pairs) line? Click **OK**.
12. Click the **Start Capture** button on the button bar and monitor for a minute or two.
13. Click the **Stop Capture** button.
14. Close **Network Monitor**. If you are asked whether to Save the capture, click **No**.


## Project 15-4

In this project, you create a trigger to make an audible sound when the capture buffer is 50% full.

**To create the trigger:**

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Network Monitor**.
2. Click the **Capture** menu and click **Trigger**.
3. For what type of events can you create a trigger? Record your observations.
4. Click the **Buffer space** radio button.
5. Click **50%** as the buffer space.
6. If it is not selected already, click **Audible Signal Only**.
7. How can you set up a trigger to execute a program?
8. Click **OK**.
9. Click the **Start Capture** button.
10. After a few minutes, click the **Stop Capture** button.
11. Leave Network Monitor open for the next assignment.


## Project 15-5

In this project, you practice obtaining baseline statistics, using Network Monitor.

**To begin gathering baselines:**

1. Make sure that Network Monitor is open, and if not, open it.
2. Click anywhere in the **Graph** pane.
3. Click the **Window** menu and click **Zoom Pane**.
4. What network statistics can you monitor from the remaining Graph pane? Record your observations.
5. Monitor for several minutes and record the typical settings for the five network performance measures. Do any of the measures seem high?
6. Close Network Monitor when you are finished. If you are asked whether to save the capture, click **No**.


## Project 15-6

In this project, you learn how to install the SNMP service and to configure a community name.

**To install the SNMP service and configure the community name:**

1. Click **Start**, point to **Settings**, and click **Control Panel**. Double-click **Add/Remove Programs**.
2. Click **Add/Remove Windows Components**. If the Windows Components Wizard dialog box is not automatically started, click the **Components** button to start it.
3. Double-click **Management and Monitoring Tools** in the Windows Components dialog box.
4. Check **Simple Network Management Protocol**, and then click **OK**.
5. Click **Next**.
6. Click **Finish**.
7. Close the Add/Remove Programs window, if it is still open.
8. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Services**.
9. Find the SNMP Service. Is it started? What is the startup type? What other service is associated with SNMP and is it started? What is its startup type?
10. Double-click **SNMP Service**.
11. Click each tab to become familiar with its contents.
12. Click the **Security** tab. What community name is already established and what rights are associated with it? Record your observations.
13. Click the **Add** button under Accepted community names.
14. Make up a community name, as you would make up a password, and enter it. Next, select **Read Write** in the Community rights box. Click the **Add** button.

15. How would you set a community name for a trap?
16. Click **OK**, and then close the Services window.


## Project 15-7

In this project, you practice using System Monitor to test a NIC to make sure that it is keeping pace with the speed of the computer in which it is installed.

**To monitor a NIC:**

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Performance**.
2. Double-click **Console Root** to view System Monitor, if it is not displayed.
3. Click **System Monitor**, if it is not already highlighted.
4. Click the **Add** (plus sign) button on the button bar.
5. Select **Network Interface** as the object to monitor.
6. Make sure that **Select counters from list** is selected and click **Output Queue Length**.
7. Select the NIC for the instance, such as **3Com EtherLink PCI**.
8. What other objects and counters might you monitor to determine the NIC's performance?
9. Click **Add** and then click **Close**.
10. To view the statistics more easily, click the **View Report** button on the button bar.
11. What is the output queue length? Is this NIC a network bottleneck?
12. When you are finished monitoring, click the **View Chart** button, and then click the **Delete** button to stop monitoring this object.


## Project 15-8

Network benchmarks are important to establish so that you can quickly identify network problems when they arise. Use this project to practice using System Monitor to gather network benchmarks on a TCP/IP-based network.



**To gather network benchmarks:**

1. Make sure that System Monitor is already open, and if it is not, open it.
2. Click the **Add** button on the button bar.
3. Select **IP** as the object to monitor.
4. Make sure that **Select counters from list** is selected and click **Datagrams Received/sec**. Click **Add**.
5. Click **Datagrams Sent/sec** as the counter and then click **Add**.
6. Click **Datagrams/sec** as the counter and then click **Add**.
7. What other objects and counters might you monitor to benchmark the server NIC's performance?

8. What counters for the TCP object should you monitor? Select these and then click **Close**.
9. Which mode—chart, histogram, or data—is best suited for monitoring this information? Record your observations.
10. Close System Monitor when you are finished monitoring.

# CASE PROJECTS


## Aspen Consulting Project: Network Monitoring

Wild Rivers is a company that manufactures canoes and kayaks for recreational use. The business and manufacturing activities of the company take place in a large industrial building that houses offices, the manufacturing unit, an inventory unit, and a shipping unit. The company supplies products to major sporting goods stores, retail outlets, and outdoor mail-order companies. Its network consists of 18 Windows 2000 Servers that are configured to use TCP/IP, and four older Novell NetWare servers that are configured for IPX/SPX. They have hired you to advise the server administrators in network monitoring, a task that has largely been ignored as the company has raced to implement servers and software to keep up with business needs.

1. The server administrators have never installed any network monitoring tools in Windows 2000 Server. Explain how to install the following:
   - Network Monitor Driver
   - Network Monitor
   - Microsoft SNMP service
2. As the next step, you emphasize the need to establish network benchmarks. Explain how to use Network Monitor and System Monitor to generate benchmarks.
3. Wild Rivers has just purchased a network management system that uses a network management station. Explain how to configure the Microsoft SNMP service on the Windows 2000 servers so that it can be used with the network management station to securely manage network devices and enable the network management station to gather SNMP-based performance information.
4. As you are working with Wild Rivers to set up SNMP, the network seems to be saturated with heavy traffic, but none of the server administrators can determine the source of the problem or if the excessive traffic is TCP/IP-based or IPX-based. Explain how they might use Network Monitor, System Monitor, or both to locate the problem. Can either of these network monitoring tools be used to monitor the NetWare servers in case they are a source of the problem, and if so, how?
5. Another problem that Wild Rivers has noticed in the past is that the network seems to respond more slowly when clients are accessing specific Windows 2000 servers. Explain how the administrators can use Network Monitor or System Monitor to determine if the root of the problem is one or more servers or the network.

## Optional Case Projects for Teams


### Team Case One

Mark Arnez is interested in developing some guidelines for network tuning that can be used by all consultants. He asks you to form a team to develop a comprehensive set of network tuning guidelines.


### Team Case Two

SNMP is a widely used network management and performance tool. Mark Arnez has an additional assignment for your team, which is to develop a document explaining the different kinds of network servers, workstations, and devices that support SNMP agent software. Use the Internet and other research sources to compile an extensive list of network equipment that supports SNMP.